

REVISTA BRASILEIRA DE POLÍTICAS PÚBLICAS BRAZILIAN JOURNAL OF PUBLIC POLICY

Sharenting, liberdade de expressão e privacidade de crianças no ambiente digital: o papel dos provedores de aplicação no cenário jurídico brasileiro

Sharenting, freedom of expression and children's privacy in the digital environment: the role of application providers under the Brazilian legal framework

Fernando Büscher von
Teschhausen Eberlin

VOLUME 7 • Nº 3 • DEZ • 2017
DIREITO E MUNDO DIGITAL

Sumário

| | |
|--|------------|
| I. INTRODUÇÃO..... | I |
| THE DATASPHERE AND THE LAW: NEW SPACE, NEW TERRITORIES | III |
| Jean-Sylvestre Bergé e Stéphane Grumbach | |
| II. DOSSIÊ ESPECIAL: DIREITO E MUNDO DIGITAL..... | 22 |
| A. CRIPTOMOEDAS E TECNOLOGIA BLOCKCHAIN | 23 |
| PASSADO, PRESENTE E FUTURO DA CRIPTOGRAFIA FORTE: DESENVOLVIMENTO TECNOLÓGICO E REGULAÇÃO..... | 25 |
| Jacqueline de Souza Abreu | |
| TRATAMENTO JURÍDICO DAS CRIPTOMOEDAS: A DINÂMICA DOS BITCOINS E O CRIME DE LAVAGEM DE DINHEIRO | 44 |
| Mariana Dionísio de Andrade | |
| TERRITÓRIO DAS CRIPTOMOEDAS: LIMITES À REGULAMENTAÇÃO ESTATAL QUANTO À CIRCULAÇÃO DE MOEDAS NO CIBERESPAÇO E POSSÍVEIS ALTERNATIVAS | 61 |
| Ranidson Gleyck Amâncio Souza | |
| CRIPTOMOEDAS E COMPETÊNCIA TRIBUTÁRIA | 80 |
| Guilherme Broto Follador | |
| BITCOIN E A (IM)POSSIBILIDADE DE SUA PROIBIÇÃO: UMA VIOLAÇÃO À SOBERANIA DO ESTADO?..... | 106 |
| Rodrigo Valente Giublin Teixeira e Felipe Rangel da Silva | |
| BLOCKCHAIN E AGENDA 2030..... | 122 |
| Danielle Mendes Thame Denny, Roberto Ferreira Paulo e Douglas de Castro | |
| A RECONSTRUÇÃO DA JURISDIÇÃO PELO ESPAÇO DIGITAL: REDES SOCIAIS, BLOCKCHAIN E CRIPTOMOEDAS COMO PROPULSORES DA MUDANÇA..... | 143 |
| Maria Edelvacy Pinto Marinho e Gustavo Ferreira Ribeiro | |
| B. PROTEÇÃO DE DADOS E PROVEDORES DE INTERNET | 158 |
| O TEMPO E O ESPAÇO. FRAGMENTOS DO MARCO CIVIL DA INTERNET: PARADIGMAS DE PROTEÇÃO DA DIGNIDADE HUMANA | 160 |
| Maria Celeste Cordeiro Leite dos Santos e Marilene Araujo | |

| | |
|---|------------|
| O PROJETO DE LEI DE PROTEÇÃO DE DADOS PESSOAIS (PL 5276/2016) NO MUNDO DO BIG DATA: O FENÔMENO DA DATAVEILLANCE EM RELAÇÃO À UTILIZAÇÃO DE METADADOS E SEU IMPACTO NOS DIREITOS HUMANOS | 185 |
| Elias Jacob de Menezes Neto, Jose Luis Bolzan de Moraes e Tiago José de Souza Lima Bezerra | |
| DIGNIDADE HUMANA NA WEBESFERA GOVERNAMENTAL BRASILEIRA..... | 200 |
| Luciana Cristina Souza | |
| CIBERESPAÇO E CONTEÚDO OFENSIVO GERADO POR TERCEIROS: A PROTEÇÃO DOS DIREITOS DE PERSONALIDADE E A RESPONSABILIZAÇÃO CIVIL DOS PROVEDORES DE APLICAÇÃO, À LUZ DA JURISPRUDÊNCIA DO SUPERIOR TRIBUNAL DE JUSTIÇA..... | 217 |
| Cristiano Colombo e Eugênio Facchini Neto | |
| A RESPONSABILIDADE CIVIL PELOS ATOS AUTÔNOMOS DA INTELIGÊNCIA ARTIFICIAL: NOTAS INICIAIS SOBRE A RESOLUÇÃO DO PARLAMENTO EUROPEU | 239 |
| Thatiane Cristina Fontão Pires | |
| Rafael Peteffi da Silva | |
| SHARENTING, LIBERDADE DE EXPRESSÃO E PRIVACIDADE DE CRIANÇAS NO AMBIENTE DIGITAL: O PAPEL DOS PROVEDORES DE APLICAÇÃO NO CENÁRIO JURÍDICO BRASILEIRO..... | 256 |
| Fernando Büscher von Teschenhausen Eberlin | |
| THE DICHOTOMY BETWEEN SMART METERING AND THE PROTECTION OF CONSUMER'S PERSONAL DATA IN BRAZILIAN LAW..... | 275 |
| Lucas Noura Guimarães | |
| O CYBERBULLYING E OS LIMITES DA LIBERDADE DE EXPRESSÃO | 295 |
| Janile Lima Viana, Cinthia Meneses Maia e Paulo Germano Barrozo de Albuquerque | |
| O SUPREMO TRIBUNAL FEDERAL E O DISCURSO DE ÓDIO NAS REDES SOCIAIS: EXERCÍCIO DE DIREITO VERSUS LIMITES À LIBERDADE DE EXPRESSÃO | 314 |
| Carlo José Napolitano e Tatiana Stroppa | |
| ANÁLISE COMPARADA DE ESTRATÉGIAS DE ENFRENTAMENTO A “REVENGE PORN” PELO MUNDO | 334 |
| Natália Neris, Juliana Pacetta Ruiz e Mariana Giorgetti Valente | |
| USO INDEVIDO DE REDES SOCIAIS E APLICATIVOS DE MENSAGENS INSTANTÂNEAS NO AMBIENTE LABORAL..... | 349 |
| Eloy Pereira Lemos Junior, Edmar Warlisson de Souza Alves e César Augusto de Castro Fiuza | |

| | |
|--|------------|
| C. DIREITO AO ESQUECIMENTO | 366 |
| ENSAIO SOBRE A PROMESSA JURÍDICA DO ESQUECIMENTO: UMA ANÁLISE A PARTIR DA PERSPECTIVA DO PODER SIMBÓLICO DE BOURDIEU | 368 |
| Joana Machado e Sergio Negri | |
| UMA AGENDA PARA O DIREITO AO ESQUECIMENTO NO BRASIL..... | 384 |
| Bruno de Lima Acioli e Marcos Augusto de Albuquerque Ehrhardt Júnior | |
| NÃO ADIANTA NEM TENTAR ESQUECER: UM ESTUDO SOBRE O DIREITO AO ESQUECIMENTO..... | 412 |
| José Augusto Fontoura Costa e Geraldo Miniuci | |
| A APLICAÇÃO DO DIREITO AO ESQUECIMENTO AOS AGENTES DELITIVOS: UMA ANÁLISE ACERCA DA PONDERAÇÃO ENTRE O DIREITO À IMAGEM E AS LIBERDADES DE EXPRESSÃO E DE INFORMAÇÃO..... | 437 |
| Paulo Afonso Cavichioli Carmona e Flávia Nunes de Carvalho Cavichioli Carmona | |
| DIREITO AO ESQUECIMENTO: NA SOCIEDADE INFORMACIONAL HÁ ESPAÇO PARA O EPÍLOGO DA MÁQUINA DE TORTURA KAFKIANA? | 454 |
| Alexandre Antonio Bruno da Silva e Marlea Nobre da Costa Maciel | |
| ESQUECIMENTO, INTERNET E “PREFERÊNCIA” DA INFORMAÇÃO: POSSIBILIDADES DE APLICAÇÃO DA DOCTRINA DOS PREFERRED RIGHTS DA JURISPRUDÊNCIA NORTE-AMERICANA AO CASO BRASILEIRO | 484 |
| Maria Vital da Rocha, Isaac Rodrigues Cunha e Karin de Fátima Rodrigues Oliveira | |
| D. PROPRIEDADE INTELECTUAL | 510 |
| DIREITOS AUTORAIS E MÚSICA: TECNOLOGIA, DIREITO E REGULAÇÃO | 512 |
| Marcia Carla Pereira Ribeiro, Cinthia Obladen de Almendra Freitas e Rubia Carneiro Neves | |
| DIREITO AUTORAL NA CIBERCULTURA: UMA ANÁLISE DO ACESSO AOS BENS IMATERIAIS A PARTIR DAS LICENÇAS CREATIVE COMMONS 4.0..... | 539 |
| Gabriela Maia Rebouças e Fernanda Oliveira Santos | |
| E. POLÍTICAS PÚBLICAS E NOVAS TECNOLOGIAS..... | 559 |
| SALTO DIGITAL NAS POLÍTICAS PÚBLICAS: OPORTUNIDADES E DESAFIOS..... | 561 |
| Marcelo D. Varella, Clarice G. Oliveira e Frederico Moesch | |
| FOSTERING E-GOVERNMENT IN BRAZIL: A CASE STUDY OF DIGITAL CERTIFICATION ADOPTION..... | 585 |
| Lamartine Vieira Braga | |
| DEMOCRATIZAÇÃO NA ERA DIGITAL: DESAFIOS PARA UM DIÁLOGO CONSCIENTE E IGUALITÁRIO..... | 602 |
| Raquel Cavalcanti Ramos Machado e Laura Nathalie Hernandez Rivera | |

REDES SOCIAIS E CROWDSOURCING CONSTITUCIONAL: A INFLUÊNCIA DA CIBERDEMOCRACIA SOBRE A GÊNESE E A INTERPRETAÇÃO DE NORMAS CONSTITUCIONAIS..... 618
Igor Ajouz

MARCO CIVIL DA INTERNET E POLÍTICA PÚBLICA DE TRANSPARÊNCIA: UMA ANÁLISE DA E-DEMOCRACIA E DO COMPLIANCE PÚBLICO 634
Juliana Costa Zaganelli e Wallace Vieira de Miranda

POLÍTICAS PÚBLICAS BRASILEIRAS DE COMPUTAÇÃO EM NUVEM: ANÁLISE DOCUMENTAL DOS RELATÓRIOS DO GLOBAL CLOUD COMPUTING SCORECARD 648
Lucas dos Santos Costa e Marcos Fernando Machado de Medeiros

O USO MONOPOLISTA DO BIG DATA POR EMPRESAS DE APLICATIVOS: POLÍTICAS PÚBLICAS PARA UM DESENVOLVIMENTO SUSTENTÁVEL EM CIDADES INTELIGENTES EM UM CENÁRIO DE ECONOMIA CRIATIVA E DE LIVRE CONCORRÊNCIA..... 672
José Antonio Remedio e Marcelo Rodrigues da Silva

1. Introdução 673
2. A urbanização das cidades e a sociedade em rede: economia criativa, colaborativa e compartilhada como formas de concretização de funções sociais da cidade..... 674
4. Concorrência e Big Data Business relevantes às Smart Cities: estudo de caso envolvendo a aquisição do Waze pelo Google 686
5. Considerações finais 689
- Referências..... 690

III. OUTROS TEMAS 694

COMO SALVAR O SISTEMA DE REPERCUSSÃO GERAL: TRANSPARÊNCIA, EFICIÊNCIA E REALISMO NA ESCOLHA DO QUE O SUPREMO TRIBUNAL FEDERAL VAI JULGAR..... 696
Luís Roberto Barroso e Frederico Montedonio Rego

PRECARIEDADE DO SISTEMA PENITENCIÁRIO BRASILEIRO COMO BASE TEMÁTICA PARA A PROIBIÇÃO OU LEGALIZAÇÃO DAS DROGAS..... 715
Lilian Rose Lemos Rocha e José Eduardo Cardozo

A TERCEIRA MARGEM DO CONSTITUCIONALISMO REPUBLICANO: UMA CRÍTICA A FRANK MICHELMAN..... 732
Daniel Barcelos Vargas

MEDIDA PROVISÓRIA E CONTROLE DE CONSTITUCIONALIDADE: RELEVÂNCIA, URGÊNCIA E PERTINÊNCIA TEMÁTICA..... 749
Clarice G. Oliveira e José Levi Mello do Amaral Júnior

| | |
|---|------------|
| OBJETO E CONCEITO DO DIREITO ADMINISTRATIVO: REVISÃO CRÍTICA..... | 765 |
| Carlos Bastide Horbach | |
| AVALIAÇÃO DE POLÍTICAS PÚBLICAS VERSUS AVALIAÇÃO DE IMPACTO LEGISLATIVO: UMA VISÃO DICOTÔMICA DE UM FENÔMENO SINGULAR | 782 |
| Aparecida de Moura Andrade e Héctor Valverde Santana | |
| LOS AVATARES DEL INTERÉS DEFINIDO EN TÉRMINOS DE PODER EN LA FORMULACIÓN DE LAS POLÍTICAS PÚBLICAS | 800 |
| Louis Valentin Mballa | |
| CONSEQUENCIALISMO JUDICIAL NA MODULAÇÃO DE EFEITOS DAS DECISÕES DECLARATÓRIAS DE INCONSTITUCIONALIDADE NOS JULGAMENTOS DE DIREITO TRIBUTÁRIO | 819 |
| Fernando Leal e Daniela Gueiros Dias | |
| JUDICIALIZAÇÃO DA SAÚDE: A DIGNIDADE DA PESSOA HUMANA E A ATUAÇÃO DO SUPREMO TRIBUNAL FEDERAL NO CASO DOS MEDICAMENTOS DE ALTO CUSTO | 845 |
| Fabrício Veiga Costa, Ivan Dias da Motta e Dalvaney Aparecida de Araújo | |

Sharenting, liberdade de expressão e privacidade de crianças no ambiente digital: o papel dos provedores de aplicação no cenário jurídico brasileiro*

Sharenting, freedom of expression and children's privacy in the digital environment: the role of application providers under the Brazilian legal framework

Fernando Büscher von Teschenhausen Eberlin**

RESUMO

Por meio das redes sociais, os pais contam suas experiências de vida e, às vezes, divulgam informações de caráter pessoal dos filhos, como fotografias, informações de localização, colégio em que estudam, rede de amigos, questões de saúde, dentre outras. Essa prática, conhecida como sharenting, cria um rastro digital que acompanha as crianças durante a vida, tem implicações no âmbito da privacidade, e coloca em rota de colisão a liberdade de expressão dos pais e a proteção dos dados pessoais dos filhos. Esse trabalho analisa essa prática e os mecanismos do Marco Civil da Internet (MCI) e da jurisprudência para endereçar tal colisão de normas. O artigo, também, analisa o papel dos provedores de aplicação, em especial redes sociais e ferramentas de busca, na criação de mecanismos que assegurem o direito ao esquecimento das crianças (a ser exercido quando entram na vida adulta) e que previnam o compartilhamento exagerado de informações pelos pais; a esse respeito, foi realizada a comparação dos modelos brasileiro e europeu, com análise normativa e jurisprudencial, objetivando encontrar elementos que auxiliem o modelo brasileiro na formulação legislativa para proteção da liberdade de expressão dos pais e da privacidade das crianças. Ao final, conclui-se pela pertinência de políticas públicas para educação em relação aos riscos do sharenting e pela necessidade de positivação de um dever de diligência dos provedores para que atuem preventivamente (melhorando a qualidade das informações sobre os riscos associados ao sharenting) e corretivamente (implementando mecanismos para efetivação do direito ao esquecimento).

Palavras-chave: Sharenting. Liberdade de Expressão. Privacidade. Direito ao Esquecimento. Proteção de Dados Pessoais.

ABSTRACT

Parents use social networks to share their own life experiences (as a father or a mother) and sometimes they also share personal information about their children, such as photographs, location, the school they study, their

* Recebido em 03/10/2017

Aprovado em 25/10/2017

** Doutorando e Mestre em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie. MBA em Ciências do Consumo Aplicadas pela Escola Superior de Propaganda e Marketing. Especialista em Direito da Responsabilidade Civil pela Direito SP (FGV). Graduado em Direito pela Universidade Presbiteriana Mackenzie. Professor do Programa de Pós Graduação Lato Sensu da Direito SP (FGV). Advogado em São Paulo. Email: fernando@eberlin.adv.br

friends network, health issues, among others. This practice, known as sharenting, creates a digital footprint that follows the child throughout his/her life, creates privacy issues and opposes parents' freedom of expression and children's personal data protection interests. The paper analyses this parental behaviour and the mechanisms to address such collision of norms under the Brazilian Internet Legal Framework (MCI) and jurisprudence. The article also examines the role of application providers, especially social networks and search engines, in the implementation of mechanisms to ensure children's right to be forgotten (to be exercised when they enter adult life) and to prevent the oversharing of information by their parents; in this particular issue, the Brazilian and European models are compared through a normative and jurisprudential analysis aiming to find elements to a legislative formulation for the Brazilian model that could ensure parents' freedom of expression as well as children's privacy. In the end, it is concluded that public policies targeting education about sharenting risks are needed, as well as the creation of a duty of care to providers in order to make them act preventively (improving the quality of information about the risks associated with sharenting) and correctively (implementing mechanisms to enforce the right to be forgotten).

Keywords: Sharenting. Freedom of expression. Privacy. Right to be forgotten. Personal data protection.

1. INTRODUÇÃO

Uma marca do mundo contemporâneo é a expressiva quantidade de informações disponíveis na rede mundial de computadores e as possíveis formas de utilização desses dados. Esse fenômeno conduz a debates jurídicos importantes ligados à privacidade, ao mau uso (ou ao uso não autorizado) de dados e à liberdade de expressão.

Em razão das implicações jurídicas decorrentes do tratamento de dados, é crescente a discussão sobre o papel, os deveres e a responsabilidade dos provedores de aplicação em relação à coleta, tratamento, e uso de informações. Uma discussão à parte nesse contexto diz respeito à responsabilidade de provedores de redes sociais e ferramentas de busca pelo conteúdo gerado por terceiros.

Este artigo irá discutir as questões acima no contexto da exposição de dados pessoais de crianças quando os pais, familiares, amigos ou mesmo pessoas ligadas a colégios e cursos frequentados por menores inserem informações a respeito destes na internet. Isso pode ocorrer nas situações mais simples como a do pai orgulhoso dos êxitos de seu filho que posta em suas redes sociais fotografias e comentários sobre atividades na escola, competições esportivas ou certificados obtidos pela criança no curso de idiomas. O compartilhamento de informações feito pelos pais na internet é denominado sharenting, conceito este que será tratado na Seção 2 deste trabalho.

A Seção 3 irá analisar a evolução das discussões referentes à colisão entre liberdade de expressão e a privacidade para associar tais debates ao contexto do sharenting. Utilizar as redes sociais para expressar aspectos da vida e das experiências da maternidade ou paternidade é um hábito dos dias atuais e constitui uma das vertentes do direito de se expressar livremente. Os pais, contudo, ao exercerem essa liberdade, expõem, sem o consentimento dos filhos, dados a respeito destes que, no futuro, podem não corresponder ao seu desejo. A liberdade de expressão dos pais, portanto, colide com interesses relativos à privacidade dos filhos, cujo incômodo com a divulgação de dados pessoais pode surgir apenas quando a criança atingir a maturidade.

Esse artigo, também, discutirá o papel dos provedores de aplicações de internet, em especial redes sociais e ferramentas de busca, para limitar a divulgação de informações de caráter pessoal de crianças. A Seção 4 irá analisar o atual contexto regulatório brasileiro em relação ao tema e a Seção 5 estudará o modelo europeu, a fim de investigar quais condutas poderiam (ou deveriam) ser adotadas pelos provedores de aplicação no contexto do sharenting.

2. O SHARENTING E OS DADOS PESSOAIS DE MENORES

Sharenting é uma expressão da Língua Inglesa que decorre da união das palavras “share” (compartilhar) e “parenting” (cuidar, no sentido de exercer o poder familiar). A prática consiste no hábito de pais ou responsáveis legais postarem informações, fotos e dados dos menores que estão sob a sua tutela em aplicações de internet. O compartilhamento dessas informações, normalmente, decorre da nova forma de relacionamento via redes sociais¹ e é realizado no âmbito do legítimo interesse dos pais de contar, livremente, as suas próprias histórias de vida, da qual os filhos são, naturalmente, um elemento central².

O problema jurídico decorrente do sharenting diz respeito aos dados pessoais das crianças que são inseridos na rede mundial de computadores ao longo dos anos e que permanecem na internet e podem ser acessados muito tempo posteriormente à publicação, tanto pelo titular dos dados (criança à época da divulgação) quanto por terceiros. Essas informações podem causar impactos desde a infância até a vida adulta e, como explica Steinberg, podem expor as crianças a constrangimentos em razão de histórias, fotografias ou comentários divulgados na web que possam ser considerados embaraçosos³. Um dado pessoal, na acepção jurídica do termo, é toda e qualquer informação que pode ser associada a uma pessoa certa, específica e determinada⁴. Exemplos clássicos são o nome ou o número de documento de alguém. Se um pai ou uma mãe expuserem na internet o nome de seus filhos (ou um número de documento ou algo que, isoladamente, permita identificá-los), eles estarão divulgando os dados pessoais da criança. Também podem ser enquadrados nesse conceito informações que, quando analisadas em conjunto, permitam identificar o titular dos dados. Informações anônimas (ou anonimizadas), tais como padrões de comportamento de um grupo de pessoas não identificáveis, não são consideradas dados pessoais.

É interessante notar que, mesmo que não haja, explicitamente, a intenção dos pais de exporem seus filhos ou, ainda, que os pais tentem exercer mecanismos para preservar os dados pessoais dos menores (omitindo o nome, por exemplo), a análise do comportamento dos adultos nas redes sociais pode permitir que terceiros façam inferências a respeito de informações que possam ser associadas a uma criança concreta e específica, tais como localização, idade, aniversário e religião⁵. Basta, para tanto, compartilhar uma recordação de viagem, de festa ou de ida à igreja em que o filho ou a filha esteja acompanhando o pai ou a mãe.

A ideia de sharenting, também, abarca as situações em que os pais fazem a gestão da vida digital de seus filhos na internet, criando perfis em nome das crianças em redes sociais e postando, constantemente, informações sobre sua rotina. É o caso da mãe que, ainda grávida, cria uma conta em uma rede social para o bebê que irá nascer. Tal rede social será alimentada com fotografias, recordações sobre aniversários, primeiros passos, primeiros dias escola, amigos, animais de estimação, relacionamento com familiares e várias outras informações. Nesse caso, os pais não estão tão somente administrando as suas próprias vidas digitais, mas também criando redes paralelas em nome de seus filhos.

1 “Typical individuals among us, even the well-educated, are technologically unsophisticated, and the cultural and economic pressures to engage in transactions that call for information disclosures are great.” ALLEN, Anita L. Protecting one’s own privacy in a big data economy. *Harvard Law Review*, v. 130, p. 71-78, dez. 2016. p. 73.

2 STEINBERG, Stacey B. Sharenting: Children’s privacy in the age of social media. *Emory Law Journal*, Atlanta, v. 66, p. 839-884, 2017. Disponível em: <<http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1796&context=facultypub>>. Acesso em: 21 ago. 2017. p. 877.

3 A autora menciona, inclusive, a existência de grupos de adultos em redes sociais que ironizam fotografias desse tipo compartilhadas por outros pais STEINBERG, Stacey B. Sharenting: Children’s privacy in the age of social media. *Emory Law Journal*, Atlanta, v. 66, p. 839-884, 2017. Disponível em: <<http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1796&context=facultypub>>. Acesso em: 21 ago. 2017. p. 854.

4 Seguindo esse conceito, o Decreto 8.771/2016, que regulamenta a Lei 12.965/2014 (Marco Civil da Internet – MCI), estabelece que dado pessoal é todo “dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa”.

5 STEINBERG, Stacey B. Sharenting: Children’s privacy in the age of social media. *Emory Law Journal*, Atlanta, v. 66, p. 839-884, 2017. Disponível em: <<http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1796&context=facultypub>>. Acesso em: 21 ago. 2017. p. 848.

A exposição exagerada de informações sobre menores pode representar ameaça à intimidade, vida privada e direito à imagem das crianças, interesses estes que são expressamente protegidos pelo art. 100, V da lei n. 8.069/1.990, o Estatuto da Criança e do Adolescente (ECA). Esse aspecto é especialmente importante porque o conceito de privacidade é contextual, temporal e depende muito do modo de vida e nível de exposição que o titular do direito está disposto a oferecer. Nesse contexto, é perfeitamente possível (senão provável) que o critério sobre privacidade que os pais possuam seja diferente daquele que a criança vai desenvolver na vida adulta. Em outras palavras, a criança pode desaprovar a conduta dos seus pais e entender que teve sua vida privada exposta indevidamente durante a infância⁶.

O exposto acima não significa, contudo, que deva existir uma proibição total e absoluta de compartilhamento, por parte dos pais, de informações referentes aos seus filhos. Primeiramente, porque cabe a eles o direito-dever de cuidar dos filhos e decidir o que é mais conveniente para as crianças em termos de vida digital e no seu melhor interesse. Além disso, deve ser considerada a liberdade de expressão dos pais de manifestar os seus próprios momentos ao lado dos filhos, mesmo que isso implique divulgar dados pessoais desses últimos.

Na maioria das vezes, não há a intenção por parte do pai ou da mãe de expor seus filhos e respectivos dados; no entanto, muitas vezes os responsáveis legais não têm conhecimento das consequências que o seu comportamento *on-line* pode causar aos menores ao longo do tempo⁷. Essa falta de compreensão das consequências da exposição de dados tem a ver com o baixo entendimento a respeito dos mecanismos da sociedade da informação⁸, que tem como um dos pressupostos a constante coleta de dados. A falta de conhecimento e de meios práticos para limitar a coleta de dados dificulta o argumento de que os pais seriam responsáveis pela excessiva exposição de informações de seus filhos⁹. Alguns exemplos da sociedade da informação mostram como a questão dos dados se torna complexa em função, por exemplo, da interação bastante constante entre os diversos tipos de mídia.

Com efeito, no mundo contemporâneo, comportamentos que outrora expunham crianças, mas que eram de certa forma controlados, não possuem, atualmente, a mesma possibilidade de controle. A esse respeito, Oswald, James e Nottingham estudaram a dinâmica de um documentário de televisão sobre a vida de crianças de 4, 5 e 6 anos. Antes do advento das redes sociais, o documentário seria exibido, repercutiria durante algum tempo, e, possivelmente, seria esquecido pela maioria das pessoas. Nos dias de hoje, no entanto, paralelamente à exibição do documentário, os telespectadores podem compartilhar comentários em redes sociais (especialmente o Twitter) a respeito das crianças que participam do programa. Tais comentários não podem ser controlados e são feitos e visualizados na internet por pessoas que não tem nenhuma relação com o círculo familiar ou de amizade dos pais. O conteúdo a respeito da criança na internet não cairá no esquecimento como o documentário televisivo, na medida em que ficará acessível na rede, podendo vir à

6 Além do aspecto da privacidade referente ao direito de não ser molestado ou de não ter a vida pessoal indevidamente exposta, também há o viés da privacidade como direito à autodeterminação informativa, ou seja, o direito de determinar o que será feito com os dados pessoais coletados no âmbito da prestação de um serviço. Esse aspecto será devidamente explorado na próxima Seção.

7 STEINBERG, Stacey B. Sharenting: Children's privacy in the age of social media. *Emory Law Journal*, Atlanta, v. 66, p. 839-884, 2017. Disponível em: <<http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1796&context=facultypub>>. Acesso em: 21 ago. 2017. p. 847.

8 “A sociedade da informação é uma nova formação política, social e econômica firmada por relações em rede, centrada na coleta, seleção, triagem e distribuição de dados por meio das tecnologias da informação. Os processos e funções essenciais em sociedade permanecem em constante e rápida transformação. E, com o advento da internet e o seu crescente uso, tornou-se ainda mais viável o exercício das liberdades atinentes ao tratamento da informação e aos modos de expressão, possibilitando ainda a imortalização e o compartilhamento de notícias e dados diversos sem limites de tempo e espaço.” MOREIRA, Rodrigo Pereira; MEDEIROS, Jaqueline Souza. Direito ao Esquecimento: Entre a Sociedade da Informação e a Civilização do Espetáculo. *Revista de Direito Privado*, v. 70, p. 71-98, 2016.

9 “The capacity of individuals qua individuals to take steps in daily life to limit Big Data's ability to capture data is limited by deficits of knowledge and practical alternatives. Holding individuals responsible for something they can do nothing about makes little sense, raising the spectre that Big Data leaves us helpless to meaningfully protect our own privacy and secure our own information.” ALLEN, Anita L. Protecting one's own privacy in a big data economy. *Harvard Law Review*, v. 130, p. 71-78, dez. 2016. p. 76.

tona anos depois¹⁰.

A sociedade da informação, também, permite que terceiros disponibilizem na internet informações pessoais de crianças como escolas que compartilham fotos em redes sociais de eventos, competições e festas envolvendo a participação de menores. No ambiente escolar, as fotografias tiradas por pais de alunos de seus filhos em eventos do colégio com outras crianças e a posterior disponibilização dessas fotografias em redes sociais é um tema muito debatido no Reino Unido e foi objeto de uma pesquisa conduzida por Bessant no ano de 2013 junto a 206 autoridades locais (“councils”) responsáveis pela gestão educação na Inglaterra, Escócia e País de Gales¹¹. O resultado encontrado aponta para o entendimento de que os pais têm o direito de fotografar seus filhos com outras crianças, desde que as fotografias se restrinjam a uma utilização pessoal. O compartilhamento das fotos na internet, contudo, é uma questão que ainda não foi respondida pela regulamentação do Reino Unido, o que causa bastante debate naqueles países¹².

As próprias crianças, também, podem gerar conteúdo que ofenda a privacidade de outros menores. O cyberbullying é uma prática que vem ganhando espaço na internet e que pode expor indevidamente informações pessoais de menores. Tal prática, de acordo com Viana, Maia e Albuquerque, é um problema de saúde pública que justifica certas limitações à liberdade de expressão¹³. Nair relata o caso extremo ocorrido em uma escola na Índia em que um menor gravou com uma câmera de celular ato sexual entre ele e sua namorada, disponibilizando o conteúdo a seus amigos, o qual, posteriormente, ficou disponível em um site de internet¹⁴.

Um último exemplo que mostra como dados pessoais de crianças podem ficar disponíveis na sociedade da informação está ligado aos mecanismos que os próprios pais usam em relação aos seus filhos, não com o objetivo de compartilhar informações, mas sim de preservar a segurança das crianças. A esse respeito, Simpson estuda o uso de equipamentos de GPS para, em nome da segurança, monitorar a localização geográfica de crianças. Tal tipo de dispositivo levanta uma série de discussões em relação à privacidade, na medida em que implica obrigar alguém (uma criança) a usar um dispositivo que gerará uma base de dados a respeito de sua localização que pode ser utilizada para diversas finalidades, inclusive comerciais¹⁵. O autor debate, ainda,

10 “They [children] can appear on social media because of the actions of others, such as parents posting photographs on a Facebook or Instagram page, or even opening a Twitter account for their baby. Where young children feature in fly-on-the-wall reality documentaries on broadcast media, however, they risk becoming the target of comment on social media outside of their immediate friends of family. This content is discoverable long after the original broadcast. We refer to them as ‘Generation Tagged’” OSWALD, Marion; JAMES, Helen; NOTTINGHAM, Emma. The not-so-secret life of five-year-olds: legal and ethical issues relating to disclosure of information and the depiction of children on broadcast and social media. *Journal Of Media Law*, v. 8, n. 2, p. 198-228, 13 out. 2016. Informa UK Limited. <http://dx.doi.org/10.1080/17577632.2016.1239942>. p. 199.

11 “The problem, however, is that when a parent takes a photograph at a school event such as a sports day or school play, it will often prove difficult for the parent to capture their child’s image alone. This is particularly the case if the parent wishes to show the child in context, and to record the child’s relationship with its peers and its involvement in the event. Whilst one might certainly accept a parent’s right to disseminate their own children’s photographs as they wish, the online dissemination of other children’s images is a very different matter.” BESSANT, Claire. Data protection, safeguarding and the protection of children’s privacy: exploring local authority guidance on parental photography at school events. *Information & Communications Technology Law*, v. 23, n. 3, p. 256-272, 2 set. 2014. Informa UK Limited. <http://dx.doi.org/10.1080/13600834.2014.973178>. p. 258.

12 BESSANT, Claire. Data protection, safeguarding and the protection of children’s privacy: exploring local authority guidance on parental photography at school events. *Information & Communications Technology Law*, v. 23, n. 3, p. 256-272, 2 set. 2014. Informa UK Limited. <http://dx.doi.org/10.1080/13600834.2014.973178>. p. 271.

13 VIANA, Janile Lima; MAIA, Cinthia MANESES; ALBUQUERQUE, Paulo Germano Barrozo de. O cyberbullying e os limites da liberdade de expressão. *Revista Brasileira de Políticas Públicas*, v. 7, n. 3, 2017.

14 “The case involved two school children in a public school in Delhi, in which a minor boy allegedly recorded his sexual act with his girlfriend in school using his camera-equipped cell phone and later transmitted it to friends. This video clip was widely circulated and eventually found its way to a popular auctions website, called bazee.com.” NAIR, Abhilash. Mobile phones and the internet: Legal issues in the protection of children. *International Review Of Law, Computers & Technology*, v. 20, n. 1-2, p. 177-185, mar. 2006. Informa UK Limited. <http://dx.doi.org/10.1080/13600860600579779>. p. 179.

15 “[...] the ability to locate individuals through such systems has led to many questions being asked about the manner in which GPS tracking can undermine privacy rights, either through compelling some persons to wear such tagging devices as well as the manner in which such tracking builds up a database of individual’s movements which may be valuable for law enforcement or commercial purposes.” SIMPSON, Brian. Tracking children, constructing fear: GPS and the manufacture of family safety. *Information*

os impactos que esse tipo de monitoramento pode trazer ao desenvolvimento da criança, que, utilizando um dispositivo tal como esse, não irá explorar os locais públicos com a mesma liberdade de alguém não monitorado¹⁶.

Os mecanismos para coleta de dados de crianças na sociedade contemporânea, como visto, são bastante amplos e os interesses sobre os dados das crianças podem ser os mais variados, desde a curiosidade, passando pelos crimes ligados à pedofilia até o objetivo de realizar práticas comerciais¹⁷.

Uma das alternativas no campo das políticas públicas para o tema, tal como sugere Steinberg, seria a implementação de medidas para educar os pais sobre o uso de mídias sociais e que reconheçam a necessidade de proteção da privacidade das crianças. A proposta permitiria não apenas aos pais, mas também a parentes, amigos, colegas e quaisquer outros terceiros que tenham relação com crianças, a aquisição de conhecimentos importantes sobre os riscos envolvidos no uso de redes sociais para compartilhar informações referentes a menores. Esse tipo de conhecimento permitiria aos pais compartilharem suas histórias de vida nas redes sociais protegendo, ao mesmo tempo, a privacidade de seus filhos¹⁸.

A proposta que este artigo objetiva aprofundar, também, envolve mecanismos de informação e educação digital, contudo sob a ótica das obrigações específicas dos provedores de aplicação de internet que, de algum modo, lidam com dados pessoais de crianças. Para traçar o caminho para essa proposta, faz-se necessário debater a atual dimensão dos direitos fundamentais à liberdade de expressão e à proteção de dados pessoais, conforme será feito na Seção 3 a seguir.

3. A COLISÃO ENTRE A LIBERDADE DE EXPRESSÃO E A PROTEÇÃO DE DADOS PESSOAIS NO CASO DO SHARENTING

A liberdade de expressão e o direito à privacidade são entendidos como direitos fundamentais, e, no âmbito das discussões referentes ao direito à privacidade, nasce, no Brasil, a ideia do direito fundamental à proteção de dados pessoais.

Sobre a liberdade de expressão, o art. 5º, IV da Constituição Federal (CF) estabelece o direito à livre manifestação do pensamento e o art. 220 da Carta Magna reforça a liberdade de informação, vedando, expressamente, a existência de dispositivos que possam constituir embaraço à liberdade de expressão jornalística ou, ainda, censura de natureza política, ideológica ou artística. Os contornos do direito à liberdade de expressão foram definidos pela jurisprudência brasileira ao longo dos anos. Um dos aspectos mais importantes dessa definição é a discussão sobre um possível caráter absoluto atribuível à liberdade de expressão.

Communications Technology Law, v. 23, n. 3, p. 273-285, 2 set. 2014. Informa UK Limited. <http://dx.doi.org/10.1080/13600834.2014.970377>. p. 274.

16 In the case of GPS tracking and important question to ask is whether such devices, often presented as liberating children through their ability to allow parents to ensure their child is safe by monitoring the child's location, actually restrict children's movements by both creating a greater fear of the public realm as well as in a practical sense allowing parents to impose and enforce more limited movement in certain areas. In this sense, the days when children explored independently may be lost if a parent can track the child's location at all times. SIMPSON, Brian. Tracking children, constructing fear: GPS and the manufacture of family safety. *Information & Communications Technology Law*, v. 23, n. 3, p. 273-285, 2 set. 2014. Informa UK Limited. <http://dx.doi.org/10.1080/13600834.2014.970377>. p. 275

17 "Collecting children's personal data may be a gold mine for online businesses who can profile children according to the details they provide with regard to their age, home town, gender, favourite cartoons, parents' occupation etc. The information collected is used to target children with advertisements relevant to their interests, and to profile them as consumers." BARTOLI, Emmanuelle. Children's data protection vs marketing companies. *International Review Of Law, Computers & Technology*, v. 23, n. 1-2, p. 35-45, jul. 2009. Informa UK Limited. <http://dx.doi.org/10.1080/13600860902742612>. p. 35.

18 STEINBERG, Stacey B. Sharenting: Children's privacy in the age of social media. *Emory Law Journal*, Atlanta, v. 66, p. 839-884, 2017. Disponível em: <<http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1796&context=facultypub>>. Acesso em: 21 ago. 2017. p. 867.

A esse respeito, um caso emblemático é o HC 82.424-2¹⁹ impetrado em favor de Siegfried Ellwanger, que tentava descaracterizar a ocorrência de crime de racismo decorrente da publicação de livros com ideias antissemitas. O Supremo Tribunal Federal (STF) analisou o direito à liberdade de expressão, entendendo que, apesar de fundamental para o Estado Democrático de Direito, este *não é absoluto* e encontra limitações nos demais direitos fundamentais²⁰. O STF reconheceu a ocorrência de uma *colisão de princípios*, especificamente a liberdade de expressão e a *dignidade*, e utilizou, na maioria dos votos proferidos nesse julgamento, a técnica do *sopesamento* com o uso do princípio da *proporcionalidade*, analisando, detidamente, o conflito no caso concreto (e não de maneira abstrata), conforme técnica que será analisada mais adiante.

Outro caso que exemplifica a construção do entendimento sobre o direito à liberdade de expressão no Brasil é o REsp n. 74.473-RJ²¹, em que os herdeiros do jogador de futebol Garrincha pleiteavam indenização de empresa cinematográfica que utilizou a imagem do jogador em um filme intitulado “Isto é Pelé”. O Superior Tribunal de Justiça (STJ) entendeu que Garrincha possui o direito sobre a sua imagem, a sua capacidade atlética e a criação do seu espírito, elementos que possuiriam um aspecto patrimonial, que pode ser defendido por seus herdeiros. Sendo o jogador um dos principais destaques do filme (“muito superior à simples coadjuvância de outros jogadores”), o Tribunal entendeu presente a ofensa ao *direito de imagem*, em conflito, no caso concreto, com a liberdade de expressão.

As características da liberdade de expressão construídas pela jurisprudência (direito não absoluto, que deve ser ponderado com o direito à dignidade, à honra e à imagem, além de outros direitos fundamentais) podem ser aplicadas à sua atual dimensão no mundo digital. Com efeito, uma das características essenciais da internet é a viabilização de espaços para que o usuário possa manifestar, de forma imediata, rápida e em padrões nunca antes imaginados, ideias e pensamentos a respeito de si próprio ou de terceiros. Por esse motivo, juntamente à proteção da privacidade, a garantia do direito à liberdade de expressão foi reconhecida no MCI como “condição para o pleno exercício do direito de acesso à internet” (art. 8º da Lei 12.965/2014).

Em relação à proteção de dados pessoais, o caráter fundamental desse direito está ligado à tutela da privacidade e à possibilidade de o rol de direitos e garantias da CF ser complementado por outros decorrentes de princípios constitucionais (§ 2º do art. 5º da CF). O art. 5º, X da CF prevê que são “invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas”. O Código Civil (CC), por seu turno, estabelece que a vida privada da pessoa natural é inviolável (art. 21), constituindo a privacidade um direito de personalidade.

A evolução histórica da legislação sobre proteção de dados demonstra a relação desse direito com a tutela da privacidade. Mendes explica essa evolução em 4 gerações de leis²². A primeira, na década de 70, era fruto da preocupação das pessoas em relação aos bancos de dados das Administrações Públicas e do poder que esses dados conferiam ao Estado sobre a vida privada dos cidadãos. Nessa fase, as leis estabeleciam procedimentos para novos bancos de dados (como a exigência de uma autorização pública prévia para criação de um sistema de armazenamento). Na segunda geração, a preocupação não era mais com os procedimentos,

19 BRASIL. Supremo Tribunal Federal. Acórdão nº 2144-3. Paciente: Siegfried Ellwanger. Relator: Ministro Maurício Corrêa. Brasília, DF, 17 de setembro de 2003. *DJ*. Brasília, 19 mar. 2004.

20 A inexistência de princípios absolutos em sistemas jurídicos que incluam direitos fundamentais se alinha com o entendimento de Alexy: “É fácil argumentar contra a existência de princípios absolutos em um ordenamento jurídico que inclua direitos fundamentais. Princípios podem se referir a interesses coletivos ou a direitos individuais. Se um princípio se refere a direitos coletivos e é absoluto, as normas de direitos fundamentais não podem estabelecer limites jurídicos a ele. Assim, até onde o princípio absoluto alcançar, não pode haver direitos fundamentais. Se o princípio absoluto garante direitos individuais, a ausência de limites desse princípio levaria à seguinte situação contraditória: em caso de colisão, os direitos de cada indivíduo, fundamentados pelo princípio absoluto, teriam que ceder em favor dos direitos de todos os indivíduos, também fundamentados pelo princípio absoluto. Diante disso, ou os princípios absolutos não são compatíveis com direitos individuais, ou os direitos individuais que sejam fundamentos pelos princípios absolutos não podem ser garantidos a mais de um sujeito de direitos.” ALEXY, Robert. *Teoria dos Direitos Fundamentais*. São Paulo: Malheiros, 2012. p.111.

21 BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 74.473-RJ. Recorrentes: Edenir dos Santos Mario e Outros. Relator: Ministro Sálvio de Figueiredo Teixeira. Brasília, DF, 25 de fevereiro de 1999. *DJ*. Brasília, 21 jun. 1999.

22 MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*. linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 37.

mas sim com normas de proteção de dados pessoais e privacidade. A terceira geração, a partir da década de 80, consagra a ideia de autodeterminação informativa, ou seja, as pessoas passam a participar do processamento de dados “como um envolvimento contínuo em todo o processo, desde a coleta, o armazenamento e a transmissão e não apenas como opção entre ‘tudo ou nada’”²³. Por fim, a quarta geração de proteção de dados introduz uma proteção maior aos chamados “dados sensíveis”²⁴ e, também, marca o surgimento de normas setoriais a respeito do assunto.

Essas gerações de leis se desenvolveram juntamente à sociedade dos dados, a qual, segundo Schreiber, traz à privacidade um significado que vai além da tradicional proteção da vida íntima, representando, também, um direito de controle sobre os dados pessoais, ou seja, o direito de a pessoa escolher se quer ou não ter as suas informações divulgadas e compartilhadas²⁵.

No caso do Sharenting, essa nova dimensão do direito à privacidade é bastante complexa. De fato, como explica Steinberg, as crianças têm interesse em proteger as informações negativas (ou até mesmo positivas) a seu respeito que foram postadas por seus pais, evitando sua disseminação sem controle, assim como podem não concordar com a decisão dos pais de compartilhar informações pessoais; contudo, as crianças não possuem uma opção de *opt-out* e nenhum tipo de controle em relação às decisões de seus pais que deixem rastros digitais²⁶. Essa falta de controle por parte dos titulares dos dados (crianças) nega o exercício do direito à autodeterminação informativa²⁷. A proteção à privacidade, nesse contexto, ganha contornos bastante complexos.

O reconhecimento da proteção de dados pessoais como direito fundamental, de acordo com Mendes, é uma “necessidade para tonar efetivos os fundamentos e princípios do Estado Democrático de Direito, na sociedade contemporânea da informação, conforme determina a Constituição Federal”²⁸. No caso específico da internet, o MCI estabeleceu, expressamente, a proteção da privacidade e dos dados pessoais como princípio do uso da internet no Brasil (art. 3º, II e III da Lei 12/965/2014), corroborando, portanto, o entendimento acima.

23 MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*. linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 42.

24 Os dados sensíveis são aqueles que se relacionam a questões muito particulares das pessoas, tais como gênero, orientação sexual, origem social e étnica, convicções políticas, orientação religiosa, questões filosóficas, dados de saúde, informações genéticas, dentre outras. No Brasil, o conceito de informação sensível foi positivado pela Lei do Cadastro Positivo (Lei n. 12.414/2011, art. 3º, § 3º, II). A problemática dos dados sensíveis está na possibilidade de seu uso para finalidades discriminatórias ou lesivas: “A coleta, armazenamento e divulgação de características como raça, credo religioso, opção sexual, política, são exemplos de condutas que afetam esses dados sensíveis, uma vez que seu uso indevido pode acarretar práticas com finalidades discriminatórias ou potencialmente lesivas, individual ou coletivamente” VIANA, Rafael Souza; SANTANA, Héctor Valverde. O compartilhamento de dados e informações pessoais de consumidores: o abuso dos fornecedores e as propostas apresentadas no PLS 181/2014. *Revista Brasileira de Políticas Públicas*, v. 7, n. 1, p. 238-253, 8 maio 2017. <http://dx.doi.org/10.5102/rbpp.v7i1.4579>. p. 246.

25 “Em uma sociedade caracterizada pelo constante intercâmbio de informações, o direito à privacidade deve se propor a algo mais que àquela finalidade inicial, restrita à proteção da vida íntima. Deve abranger também o direito da pessoa humana de manter o controle sobre os seus dados pessoais. Mais sutil, mas não menos perigosa que intromissão na intimidade doméstica de uma pessoa, é a sua exposição ao olhar alheio por meio de dados fornecidos ou coletados de forma aparentemente inofensiva, no preenchimento de um cadastro de hotel ou no acesso a um site qualquer.” SCHREIBER, Anderson. *Direitos da Personalidade*. São Paulo: Atlas, 2011. p. 129. Mais adiante, o autor conclui: “Como se vê, a tutela da privacidade, nessa nova acepção, não se contenta com a proibição à intromissão alheia na vida íntima (dever geral de abstenção). Impõe também deveres de caráter positivo, como o dever de solicitar autorização para a inclusão do nome de certa pessoa em um cadastro de dados ou o dever de possibilitar a correção de dados do mesmo cadastro pelo seu titular, a qualquer tempo.” SCHREIBER, Anderson. *Direitos da Personalidade*. São Paulo: Atlas, 2011. p. 131.

26 STEINBERG, Stacey B. Sharenting: Children’s privacy in the age of social media. *Emory Law Journal*, Atlanta, v. 66, p. 839-884, 2017. Disponível em: <<http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1796&context=facultypub>>. Acesso em: 21 ago. 2017. p. 843.

27 O princípio da autodeterminação informativa significa ter o poder de determinar o que será feito com os dados pessoais eventualmente fornecidos, assim como ter o direito de ter os dados utilizados apenas para a finalidade para a qual foram coletados. No Direito Brasileiro, esse princípio foi positivado pela Lei 12.414/2011 (Lei do Cadastro Positivo) no art. 5º, VII.

28 MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*. linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 172.

Seguindo essa tendência, o caráter fundamental do direito à proteção de dados foi expressamente reconhecido na legislação comunitária europeia, por meio do Regulamento 2016/679²⁹, que considera a proteção de dados como um direito fundamental (arts. 1º e 2) que deve ser equilibrado com outros direitos fundamentais em conformidade com o princípio da proporcionalidade.

No caso do sharenting, portanto, há dois interesses em colisão. De um lado, os direitos fundamentais à privacidade e à proteção de dados pessoais das crianças e, do outro, o direito à liberdade de expressão dos pais (e, eventualmente de terceiros - colégio, amigos) no ambiente digital.

O conflito entre as normas que regulam tais direitos deve ser endereçado por meio de técnicas de ponderação. Alexy explica que as normas são classificadas como regras ou princípios. As regras devem ser analisadas como normas que impõem condutas (ou proibição de condutas) e que devem ser aplicadas a um determinado caso concreto na *exata maneira como formuladas*; nem mais, nem menos³⁰. Se duas regras entrarem em conflito, uma delas deve ser declarada inválida e os critérios a serem utilizados para a solução desse conflito são os da “*lex posterior derogat priori* e *lex specialis derogat legi generali*”³¹. O conflito entre regras, portanto, ocorre na dimensão da validade das normas, ou seja, uma regra será válida e a outra não. Os princípios, por seu turno, são “normas que ordenam que algo seja realizado na maior medida possível dentro das possibilidades jurídicas e fáticas existentes”³². Em outras palavras, os princípios são mandamentos de otimização, normas de maior generalidade, que, quando analisadas isoladamente, podem levar a resultados diferentes em uma mesma situação concreta. Os princípios em colisão devem ser sopesados com base na máxima da proporcionalidade, ou seja, deverá haver a relativização dos princípios em face das possibilidades jurídicas em cada caso concreto³³.

Ainda em relação ao conflito entre direitos fundamentais, Canaris reconhece que “pertence à essência dos princípios gerais de Direito que eles entrem, com frequência, em conflito entre si, sempre que, tomados em cada um, apontem soluções opostas”. Nesse contexto, para se trabalhar com as aparentes contradições/oposições de princípios e valores, deve-se lançar mão de ferramentas tais como a interpretação sistemática, ou seja, interpretar uma norma ou uma situação entendendo o sentido de cada princípio para o sistema e buscando uma solução, no caso concreto, que faça valer esse sentido³⁴.

A análise sobre os direitos a serem tutelados no caso do sharenting demanda mecanismos de solução para os casos concretos (seja pela ponderação com base no princípio da proporcionalidade, seja com base na interpretação sistemática), sendo necessário encontrar uma justa medida para preservar tanto o direito à liberdade de expressão dos pais e de terceiros como o direito à privacidade e à proteção de dados pessoais de crianças. Como visto nos exemplos acima, o uso desse tipo de mecanismo não é novo na jurisprudência brasileira e pode ser perfeitamente aplicado aos casos de conflitos entre princípios na sociedade da informação.

Nesse cenário, a atuação das aplicações de internet pode contribuir para que se alcance a melhor solução, uma vez que, em relação ao sharenting, a questão da proteção dos dados pessoais (e, também, da privacidade) das crianças surge quando os seus pais postam informações a seu respeito *por meio de aplicações* que funcionam como uma espécie de *intermediário* para divulgação dos dados. Havendo um caráter potencialmente lesivo nos serviços fornecidos pelos provedores de internet, é necessário entender se existe e quais seriam os critérios de responsabilidade dessas aplicações, assim como quais seriam os direitos e deveres de tais intermediários no âmbito de sua prestação de serviços. A análise sobre o papel dos provedores de aplicação será efetuada na próxima Seção.

29 Regulamento (UE) do Parlamento Europeu e do Conselho nº 2016/679, de 27 de abril de 2016, Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <<http://eur-lex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:32016R0679&from=en>>. Acesso em: 28 ago. 2017.

30 ALEXY, Robert. *Teoria dos Direitos Fundamentais*. São Paulo: Malheiros, 2012. p. 91.

31 ALEXY, Robert. *Teoria dos Direitos Fundamentais*. São Paulo: Malheiros, 2012. p. 93.

32 ALEXY, Robert. *Teoria dos Direitos Fundamentais*. São Paulo: Malheiros, 2012. p. 90.

33 ALEXY, Robert. *Teoria dos Direitos Fundamentais*. São Paulo: Malheiros, 2012. p. 117.

34 CANARIS, Claus-Wilhelm. *Pensamento Sistemático e Conceito de Sistema na Ciência do Direito*. 3. ed. Lisboa: Fundação Calouste Gulbenkian, 2002. p. 205.

4. A RESPONSABILIDADE DOS PROVEDORES DE APLICAÇÃO PELO CONTEÚDO GERADO POR TERCEIROS E O ATUAL O MODELO BRASILEIRO

Uma aplicação de internet, de acordo com o MCI, é o “conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet” (art. 5º, VII, da Lei 12.965/2014). Um provedor de aplicações, portanto, é aquele que dá acesso a esse conjunto de funcionalidades.

Analisando-se o contexto europeu e a possível responsabilidade dos provedores de aplicação pelo conteúdo gerado por terceiros, Erdos³⁵ elenca três espécies de provedores: (i) o mero processador de informações, que armazena e comunica dados de terceiros, como um provedor de hospedagem (*processor host*); (ii) o processador de informações que, além de armazenar e comunicar dados de terceiros, também, é um controlador desses dados, na medida em que trabalha a forma de comunicação das informações, como ocorre com o Facebook e o Youtube (*controller host*) e (iii) o intermediário, que desenvolve suas atividades de maneira independente do detentor dos dados, como é o caso de sites de avaliação e de ferramentas de busca especializadas (*independent intermediary*). Em função do tipo de atividade que desenvolvem, os provedores teriam responsabilidades maiores ou menores em relação ao conteúdo gerado por terceiros.

Na primeira situação (*processor host*), o provedor que simplesmente publica informações obedecendo instruções de um terceiro não ficaria, a princípio, sujeito à responsabilidade civil, pois não possui ingerência em relação às informações armazenadas no website hospedado, não fazendo, ademais, nenhuma atividade de tratamento de dados pessoais³⁶. No caso do sharenting, seria a hipótese do provedor que hospeda um site feito por um pai que insere na página de internet por ele criada dados pessoais de seu filho. O pai, dono do site, pode vir a ser responsabilizado, mas o provedor de hospedagem não.

Já o *controller host* possui alguns deveres de cuidado em relação aos dados pessoais. Isso ocorre porque esse tipo de provedor efetua uma atividade de tratamento das informações (determinando, por exemplo, a forma como os dados serão comunicados a terceiros, como ocorre com as redes sociais), o que impõe a eles o dever de adotar medidas razoáveis todas as vezes que tomarem conhecimento da postagem de conteúdo ilegal ou inadequado³⁷. Também pode ser entendido que esses provedores possuem deveres preventivos, tais como possuir código de conduta para os seus usuários e políticas sobre dados pessoais, ou ainda medidas concretas como bloquear, através de mecanismos automatizados, conteúdo claramente contrário às suas políticas (pornografia infantil, por exemplo). Em relação ao sharenting, pode-se pensar nas redes sociais que divulgam as postagens feitas pelos pais contendo informações a respeito de seus filhos. O papel das redes sociais é importante na medida em que criam *expectativas de segurança* nos pais que as utilizam. Para exemplificar, Steinberg explica que aplicações como o Facebook oferecem ao usuário a possibilidade de escolher as pessoas que poderão ver cada postagem realizada, o que cria uma falsa sensação de que os dados compartilhados não serão vistos por mais pessoas além daquelas delimitadas pelo usuário; contudo, mesmo as postagens “controladas”, podem ser compartilhadas e vistas por um público muito mais amplo do que o

35 ERDOS, David. Delimiting the Ambit of Responsibility of Intermediary Publishers for Third Party Rights in European Data Protection: Towards a Synthetic Interpretation of the EU acquis. *University of Cambridge Faculty of Law Research Paper No. 31/2017*, Cambridge, 27 jun. 2017. Disponível em: <<https://ssrn.com/abstract=2993154>>. Acesso em: 21 ago. 2017. p. 21.

36 “Processors are not directly responsible for ensuring adherence to substantive data protection standards, a position which is maintained in Regulation 2016/679” (ERDOS, David. Delimiting the Ambit of Responsibility of Intermediary Publishers for Third Party Rights in European Data Protection: Towards a Synthetic Interpretation of the EU acquis. *University of Cambridge Faculty of Law Research Paper No. 31/2017*, Cambridge, 27 jun. 2017. Disponível em: <<https://ssrn.com/abstract=2993154>>. Acesso em: 21 ago. 2017. p. 22.

37 “[...] requirements to vindicate rights *ex post* may, following a data subject contacting them about a data protection concern, require ‘controller hosts’ to take reasonable steps to detect the precise processing at issue, undertake a *bona fide* assessment of its legality and sometimes event to adopt continuing measures to prevent the repetition of specific illegalities.” ERDOS, David. Delimiting the Ambit of Responsibility of Intermediary Publishers for Third Party Rights in European Data Protection: Towards a Synthetic Interpretation of the EU acquis. *University of Cambridge Faculty of Law Research Paper No. 31/2017*, Cambridge, 27 jun. 2017. Disponível em: <<https://ssrn.com/abstract=2993154>>. Acesso em: 21 ago. 2017. p. 25.

inicialmente imaginado³⁸.

Por fim, no caso dos intermediários (*independent intermediaries*), por não efetuarem armazenamento e publicação de informações sob as instruções de terceiros, estes não possuem, num primeiro momento, os argumentos para isenção de responsabilidade que o *processor host* possui. Esses intermediários coletam e tratam informações por conta própria, o que pode aumentar o seu nível de responsabilidade caso as informações tratadas divulguem dados pessoais de terceiros. Um exemplo mencionado por Erdos³⁹ seria a situação de uma ferramenta de busca especializada em obter informações de caráter personalíssimo, como números de documentos, de cartões de crédito, de telefone ou informações de contato como um *e-mail*⁴⁰. Tais provedores devem observar todas regras e deveres de conduta, preventivos e corretivos, inerentes à proteção de dados pessoais⁴¹. Para o sharenting, pode-se imaginar sites especializados em coletar e divulgar informações sobre crianças geradas por terceiros (uma maternidade, por exemplo, que filtre e divulgue dados sobre bebês ali nascidos postados pelos respectivos pais em redes sociais).

A classificação acima ajuda a entender a natureza dos serviços prestados por provedores de aplicações e o nível de responsabilidade que eles deveriam possuir em função desses serviços. No atual contexto brasileiro, no entanto, a experiência decorrente da legislação e jurisprudência aponta para um caminho de pouca responsabilidade dos provedores de aplicação em relação ao conteúdo gerado por terceiros, não importando muito a natureza das atividades que realizam. Com efeito, o MCI estabeleceu a regra segundo a qual os provedores de aplicação somente serão responsabilizados se deixarem de cumprir ordem judicial específica, “no âmbito e nos limites técnicos de seu serviço” (art. 19 da Lei 12.965/2014). No caso específico de o conteúdo gerado por terceiros conter imagens, vídeos ou outros materiais “contendo cenas de nudez ou de atos sexuais de caráter privado”, o provedor deve adotar medidas imediatas, independentemente de ordem judicial, mas ainda sim “no âmbito e nos limites técnicos de seu serviço” (art. 21 da Lei 12.965/2014)⁴². Para o sharenting, isso significa que os websites só estariam obrigados a adotar medidas independentemente de ordem judicial em casos extremos como os de pedofilia⁴³.

38 STEINBERG, Stacey B. Sharenting: Children’s privacy in the age of social media. *Emory Law Journal*, Atlanta, v. 66, p. 839-884, 2017. Disponível em: <<http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1796&context=facultypub>>. Acesso em: 21 ago. 2017. p. 850.

39 ERDOS, David. Delimiting the Ambit of Responsibility of Intermediary Publishers for Third Party Rights in European Data Protection: Towards a Synthetic Interpretation of the EU acquis. *University of Cambridge Faculty of Law Research Paper No. 31/2017*, Cambridge, 27 jun. 2017. Disponível em: <<https://ssrn.com/abstract=2993154>>. Acesso em: 21 ago. 2017. p. 27.

40 Um exemplo nesse sentido é o site <<http://www.consultasocio.com/>> (acesso em: 30 ago. 2017), que fornece informações detalhadas sobre empresas nas quais pessoas físicas sejam sócias ou administradoras. Outro exemplo seriam alguns sites de avaliação que armazenam informações sobre terceiros sem que eles necessariamente saibam e possam controlar a veracidade dessas informações.

41 “[...] such independent intermediaries should simply fulfil all the controller obligations as set down in European data protection law [...] this would entail a comprehensive *ex ante* and *ex post* responsibility for ensuring that data met all substantive benchmarks including, for example, as regards data accuracy and restrictions around the processing of sensitive personal data.” ERDOS, David. Delimiting the Ambit of Responsibility of Intermediary Publishers for Third Party Rights in European Data Protection: Towards a Synthetic Interpretation of the EU acquis. *University of Cambridge Faculty of Law Research Paper No. 31/2017*, Cambridge, 27 jun. 2017. Disponível em: <<https://ssrn.com/abstract=2993154>>. Acesso em: 21 ago. 2017. p. 27.

42 A respeito da evolução da jurisprudência do STJ em relação ao tema, tanto antes como depois do MCI, o estudo de Colombo e Facchini Neto demonstra que ela se mantém estável no sentido de garantir uma ampla liberdade de expressão e de preservar a atividade dos provedores de aplicação, os quais, historicamente, mesmo antes do MCI, vinham respondendo subjetivamente perante as pessoas ofendidas por conteúdo gerado por terceiros. COLOMBO, Cristiano; FACCHINI NETO, Eugênio. Ciberespaço e conteúdo ofensivo gerado por terceiros: a proteção dos direitos de personalidade e a responsabilização civil dos provedores de aplicação, à luz da jurisprudência do Superior Tribunal de Justiça. *Revista Brasileira de Políticas Públicas*, v. 7, n. 3, 2017.

43 Tal regra cria uma espécie de escudo legal para os prestadores de serviço no âmbito da internet. Em primeiro lugar, porque subordina as providências a serem tomadas pelos provedores aos *limites técnicos* de seus serviços, o que, muitas vezes, pode permitir argumentos de isenção de responsabilidade por parte dos provedores, que possuem, cada qual, questões técnicas específicas inerentes aos seus serviços. Além disso, ressalvadas as hipóteses de “cenas de nudez ou de atos sexuais de caráter privado”, tais provedores somente serão responsabilizados pelo conteúdo gerado por terceiros se deixarem de cumprir uma ordem judicial específica. Essa regra proporciona um ambiente cômodo para o prestador de serviço que tem um critério objetivo (ordem judicial) para lidar com as situações concretas; contudo, do outro lado da moeda, a norma conduz a demandas judiciais que poderiam ser evitadas com o tratamento das situações diretamente pelos provedores.

O AgInt no REsp n. 1.593.873-SP⁴⁴ é um caso emblemático a respeito do entendimento do Superior Tribunal de Justiça (STJ) sobre a (ausência de) responsabilidade de provedores de aplicação pelo conteúdo gerado por terceiros. No caso específico, foi analisada a responsabilidade das ferramentas de busca. Em síntese, a Google levou ao STJ discussão surgida na ação ajuizada por “SMS” para eliminar resultados de busca que envolvessem o nome da autora da ação, já que tais buscas poderiam levar a sites contendo imagens de nudez da mesma. Nesse caso, um dos direitos colocados em julgamento era o “direito ao esquecimento”, que foi entendido como importante para a preservação da privacidade “quando as circunstâncias assim determinarem”. Ao analisar a atividade desenvolvida pelas ferramentas de busca e suas peculiaridades técnicas, o STJ entendeu que os danos decorrentes do resultado das buscas realizadas pelos usuários não poderiam ensejar a responsabilização do provedor desse serviço. Nos termos do acórdão, a ferramenta de busca é parte ilegítima para esse tipo de pedido, sendo que o ofendido deveria buscar medidas tendentes à supressão do conteúdo ofensivo diretamente perante aquele que disponibiliza esse conteúdo na rede e não perante o site de pesquisas. Um dos aspectos bastante acentuados nessa decisão é o fato de o Brasil não possuir uma legislação geral para proteção de dados pessoais.

O caso descrito acima é marcante na jurisprudência brasileira, pois não reconhece que a ferramenta de busca seja uma entidade responsável pelo tratamento de dados, já que estes foram colocados na internet por terceiros. O mesmo tipo de raciocínio, se trazido para a discussão envolvendo o sharenting, permitiria ao provedor de aplicação alegar a impossibilidade técnica de controlar as informações que os pais colocam na internet a respeito de seus filhos, ainda que as informações referentes à infância possam ficar no algoritmo de busca do Google por muitos anos, revelando-se de maneiras embaraçosas durante toda a vida da criança⁴⁵.

O entendimento em relação ao tema no direito comunitário europeu aponta para o caminho da existência de deveres, fundamentados no direito ao esquecimento, por parte dos provedores de aplicação, inclusive ferramentas de busca, em relação ao conteúdo gerado por terceiros. Esse entendimento será detalhado na próxima Seção.

5. O MODELO EUROPEU BASEADO NO DIREITO AO ESQUECIMENTO E AS ALTERNATIVAS PARA O MODELO BRASILEIRO

Comparando-se o modelo brasileiro acima descrito com o europeu, nota-se que há um rigor mais elevado no velho continente em relação à responsabilidade pela inserção de dados de terceiros na rede mundial de computadores.

O maior rigor do modelo europeu é bem ilustrado no caso “Lindqvist”⁴⁶. No referido precedente, a Sra. Lindqvist, além de exercer suas atividades profissionais, era catequista numa Paróquia na Suécia. Certa vez, em 1998, no âmbito de um curso de informática que havia frequentado, resolveu desenvolver uma página de internet, em sua casa, com seu computador, para que os paroquianos pudessem obter informações eventualmente necessárias para prepararem a crisma. Nesse site, a Sra. Lindqvist inseriu informações pessoais a seu respeito e a respeito de mais 18 colegas da Paróquia, incluindo nomes, hobbies, funções ocupadas na

44 BRASIL. Superior Tribunal de Justiça. AgInt no Recurso Especial n. 1.593.873-SP. Agravante: Google Brasil Internet Ltda. Relatora: Ministra Nancy Andrighi. Brasília, DF, 10 de novembro de 2016. *DJe*. Brasília, 17 nov. 2016.

45 STEINBERG, Stacey B. Sharenting: Children’s privacy in the age of social media. *Emory Law Journal*, Atlanta, v. 66, p. 839-884, 2017. Disponível em: <<http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1796&context=facultypub>>. Acesso em: 21 ago. 2017. p. 868.

46 UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. *Acórdão n.º C-131/12*. Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González. Luxemburgo, 2014. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT>>. Acesso em: 09 set. 2017.

atividade paroquial, estado civil e número de telefone. A Sra. Lindqvist não avisou os colegas da existência do site e, além disso, solicitou ao administrador da página de internet da igreja que fizesse um link para o site criado por ela. Assim que soube que alguns dos colegas não estavam satisfeitos com a página, a Sra. Lindqvist a retirou do ar. Por essa razão, a paroquiana foi processada por tratar dados de caráter pessoal sem obter a autorização dos seus titulares e sem avisar a autoridade de controle sueca. O Tribunal de Justiça da União Europeia entendeu que a disponibilização de informações de caráter pessoal da internet, deixando-as acessíveis a todos, mesmo na peculiar situação da Sra. Lindqvist (site particular, sem finalidades econômicas, feito no âmbito de uma atividade benevolente), constitui tratamento de dados⁴⁷. Essa decisão foi um dos marcos para a construção de um conceito amplo sobre o que é *tratamento* de dados pessoais e tem o efeito prático de impor as obrigações da legislação de proteção de dados às mais singelas atividades que tragam qualquer tipo de divulgação de informações de caráter pessoal.

Ainda no âmbito no Direito Europeu, é emblemático o caso conhecido como “Google Spain”⁴⁸. Aqui, o autor da ação, Sr. Mario Costeja González, afirmava que, quando pesquisado o seu nome, a ferramenta de buscas da Google apresentava duas páginas do jornal La Vanguardia do ano de 1998 com informações sobre a venda de imóveis decorrente de um arresto em função de dívidas que este possuía. Aduz que o processo de arresto já havia sido resolvido há vários anos e que não havia pertinência na referência ao mesmo no site de busca, motivo pelo qual requereu que seus dados pessoais deixassem de aparecer nos resultados de pesquisa associados aos fatos acima narrados. A Google, por seu turno, alegou não ter controle sobre o conteúdo postado por terceiros e que o Autor deveria adotar as providências que entendesse pertinentes diretamente junto ao site que publicou as informações. O Tribunal de Justiça da União Europeia entendeu que a atividade realizada pela Google se enquadra no conceito de tratamento de dados pessoais, estando sujeita às obrigações respectivas, dentre as quais se encontram a de assegurar a correção e exatidão dos dados. O Tribunal, também, analisou a necessidade de sopesar os interesses do autor e os da coletividade, especialmente daqueles que, por qualquer motivo, queiram ter acesso à informação. Nesse aspecto, a conclusão alcançada foi no sentido de reconhecer o direito ao esquecimento no caso concreto por não haver razões especiais que justificassem um interesse preponderante da coletividade na informação referente às dívidas já quitadas pelo Sr. Costeja González.

O reconhecimento do direito ao esquecimento pelo Tribunal de Justiça da União Europeia e da obrigação de o provedor de aplicações adotar medidas para efetivar esse direito é um indicativo importante para a proteção dos interesses das crianças no sharenting. Com efeito, como afirma Steinberg, o reconhecimento do direito ao esquecimento pode ser uma alternativa para encontrar o justo equilíbrio entre a proteção da privacidade da criança e a liberdade de expressão dos pais. De acordo com a autora, quando um pai ou uma mãe compartilham informações sobre o seu filho ou filha *on-line*, eles têm o objetivo de expressar questões ligadas, exclusivamente, ao crescimento dos filhos e ao seu momento de vida como pai ou mãe. Esse objetivo perde o propósito com o crescimento da criança, de modo que a imposição da obrigação de apagar os dados pessoais de crianças ou desindexá-los de sites de busca com o passar do tempo assegura, ao mesmo tempo, o direito dos pais de se manifestarem em relação ao crescimento de seus filhos e os interesses das crianças em relação aos seus dados pessoais⁴⁹.

Embora não esteja positivado de maneira clara, o direito ao esquecimento é reconhecido pela doutrina

47 A Sra. Lindqvist, também, foi acusada de ter transferido dados pessoais para outros países sem autorização dos seus titulares, na medida em que os disponibilizou na rede mundial de computadores, de modo que pudessem ser acessados por residentes em outros países. Sobre esse aspecto, o Tribunal entendeu que a acusação não procedia, pois o site e os dados pessoais estavam hospedados dentro do próprio Estado ou de um Estado Membro.

48 UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. *Acórdão n.º C-131/12. Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González*. Luxemburgo, 2014. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT>>. Acesso em: 09 set. 2017.

49 STEINBERG, Stacey B. Sharenting: Children’s privacy in the age of social media. *Emory Law Journal*, Atlanta, v. 66, p. 839-884, 2017. Disponível em: <<http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1796&context=facultypub>>. Acesso em: 21 ago. 2017. p. 876.

brasileira. Chehab o conceitua como “a faculdade que o titular de um dado ou fato pessoal tem para vê-lo apagado, suprimido ou bloqueado, pelo decurso do tempo e por afrontar seus direitos fundamentais”⁵⁰. Lima reconhece o direito ao esquecimento como um direito de personalidade “através do qual o indivíduo pode excluir ou deletar as informações a seu respeito quando tenha passado um período de tempo desde a sua coleta e utilização e desde que não tenham mais utilidade ou não interfiram no direito de liberdade de expressão [...]”⁵¹. Moreira e Medeiros enxergam no direito ao esquecimento um direito fundamental⁵². Acioli e Erhardt Júnior entendem que algumas facetas do direito ao esquecimento estão presentes no MCI (como o direito à exclusão dos dados pessoais - art. 7º - e o direito à remoção de conteúdo gerado por terceiros que divulgue, sem autorização, materiais contendo cenas de nudez ou de atos sexuais de caráter privado - art. 21)⁵³. Rocha, Cunha e Oliveira, por seu turno, propõem critérios para aplicação do direito ao esquecimento com base na teoria estadunidense da “posição privilegiada de direitos”⁵⁴.

O Regulamento 2016/679 da União Europeia⁵⁵, no artigo 17, 1, “f” positivou esse direito, inclusive, no âmbito do *sharenting*, ao facultar ao titular dos dados pessoais o direito de apagamento de suas informações quando elas forem coletadas durante a infância. Essa obrigação imposta aos provedores de aplicação tende a assegurar o direito à autodeterminação informativa da criança ao atingir a maturidade, além de preservar sua privacidade e o direito à liberdade de expressão dos pais.

No atual contexto brasileiro, contudo, essa alternativa demandaria uma evolução no atual posicionamento da jurisprudência em relação às obrigações dos provedores pelo conteúdo gerado por terceiros. Considerando-se, no entanto, que o direito ao esquecimento é reconhecido pela doutrina e que o mundo digital possui aspectos específicos que colocam as crianças em situação de hipervulnerabilidade⁵⁶, uma análise diferenciada do tema em relação aos produtos e serviços que tenham algum impacto sobre o público infantil é absolutamente coerente com o ordenamento pátrio.

Nessa linha, vale ressaltar que o direito brasileiro possui normas estabelecendo obrigações de cuidado em relação às crianças (art. 227 da CF e art. 100, V do ECA), obrigações de prestar informações claras e

50 CHEHAB, Gustavo Carvalho. O direito ao esquecimento na sociedade da informação. In: CLÈVE, Clèmerson Merlin. *Dout-rinas Essenciais de Direito Constitucional*. São Paulo: Revista dos Tribunais, 2015. p. 563-596.

51 LIMA, Cíntia Rosa Pereira de. Direito ao Esquecimento e Internet: o fundamento legal no Direito Comunitário europeu, no Direito italiano e no Direito brasileiro. *Revista dos Tribunais*, v. 946, p.77-109, ago. 2014.

52 “o direito ao esquecimento surgiu como um aspecto da privacidade, projetando o direito de ser deixado em paz e recair no esquecimento e no anonimato após certo decurso de tempo atinente a um evento público envolvendo pessoa pública ou não. O dever de memória é inválido se não for justificado em necessidades históricas, assim, o direito ao esquecimento será imposto a todos e em benefício de todos. Esse direito é independente, sendo uma tutela da memória individual e da memória coletiva. Trata-se de um direito fundamental e essencial ao livre desenvolvimento da personalidade humana” MOREIRA, Rodrigo Pereira; MEDEIROS, Jaqueline Souza. Direito ao Esquecimento: Entre a Sociedade da Informação e a Civilização do Espetáculo. *Revista de Direito Privado*, v. 70, p. 71-98, 2016.

53 ACIOLI, Bruno de Lima; EHRHARDT JÚNIOR, Marcos Augusto de Albuquerque. Uma agenda para o direito ao esqueci-mento no Brasil. *Revista Brasileira de Políticas Públicas*, v. 7, n. 3, 2017.

54 Ao analisar o conflito entre a liberdade de expressão e o direito ao esquecimento no âmbito da internet, os autores propõem que a liberdade de expressão pode prevalecer sobre o direito ao esquecimento somente quando forem preenchidos requisitos que denotem uma perspectiva cívica na divulgação das informações (veracidade, zelo na apresentação dos fatos, relevância histórica, científica e social do que se está divulgando, preservação do nome dos envolvidos e respeito à dignidade humana). ROCHA, Maria Vital da; CUNHA, Isaac Rodrigues; OLIVEIRA, Karin de Fátima Rodrigues. Esquecimento, internet e “preferência” da infor-mação: possibilidades de aplicação da doutrina dos preferred rights da jurisprudência norte-americana ao caso brasileiro. *Revista Brasileira de Políticas Públicas*, v. 7, n. 3, 2017.

55 Regulamento (UE) do Parlamento Europeu e do Conselho nº 2016/679, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <<http://eur-lex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:32016R0679&from=en>>. Acesso em: 28 ago. 2017.

56 “A hipervulnerabilidade do consumidor criança e adolescente é mais patente com o desenvolvimento das novas tecnologias, como a Internet, telefones celulares de última geração, videogames, aparelhos digitais etc. A velocidade das informações tornou-se muito mais rápida nos últimos vinte anos e hoje nossas crianças e adolescentes têm acesso mais facilitado aos bens de consumo, o que demonstra a necessidade de maior proteção em relação a estes consumidores.” NISHIYAMA, Adolfo Mamoru; DENSA, Rob-erta. A Proteção dos Consumidores Hipervulneráveis: os portadores de deficiência, os idosos, as crianças e os adolescentes. *Revista de Direito do Consumidor*, v. 76, p. 13-45, out./dez. 2010.

precisas sobre os serviços contratados e seus riscos, com base na boa-fé (art. 31 do CDC e art. 113 do CC) e obrigações de reparar danos (arts. 6º, VI e 7º, § único do CDC e 927 do CC). Uma análise teleológica desse arcabouço normativo, com base nos argumentos expostos ao longo desse texto, pode, perfeitamente, conduzir a duas espécies de obrigações.

A primeira seria uma obrigação de caráter preventivo, ou seja, de melhorar a qualidade das informações sobre os serviços oferecidos, inclusive e especialmente, os riscos associados ao compartilhamento de dados. Esse cuidado deve ser redobrado quando o provedor detectar a possibilidade de compartilhamento de informações de crianças. As redes sociais, por exemplo, poderiam aumentar o nível de informações transmitidas aos pais, alertando-os sobre os riscos relativos ao sharenting, evitando o surgimento da falsa sensação de segurança já mencionada acima. De um ponto de vista prático, essa tarefa não se mostra tão complicada. Pode-se imaginar, por exemplo, que todos os usuários de uma rede social, ao preencherem o seu cadastro, informem se possuem filhos e se pretendem compartilhar informações a respeito dos mesmos. Caso a resposta do usuário seja afirmativa, informações específicas sobre esses riscos, transmitidas de forma clara e destacada do contrato padrão, lhes seriam transmitidas. O importante é que os mecanismos de informação sejam concebidos de modo a fazer com que os pais, efetivamente, leiam o seu conteúdo⁵⁷.

O segundo tipo de medida que pode ser adotada no atual contexto da legislação brasileira é de caráter corretivo. Como as crianças não possuem qualquer controle sobre os dados que seus pais (ou terceiros) postam a seu respeito, o exercício de direitos inerentes à autodeterminação informativa depende da disponibilização de mecanismos que permitam o apagamento de dados a seu respeito que foram postados por terceiros ao longo da infância⁵⁸. Trata-se da concretização da autodeterminação informativa por meio do direito ao esquecimento. Esse tipo de obrigação pode ser imposto tanto aos provedores nos quais o conteúdo é postado (redes sociais) como às ferramentas de busca. Em relação a essas últimas, apesar de a jurisprudência brasileira, como demonstrado na Seção 4, entender que não cabe às ferramentas de busca a exclusão de resultados de pesquisa com conteúdo gerado por terceiros, a hipervulnerabilidade das crianças justifica, ao menos nessa hipótese concreta, uma maior reflexão a respeito do tema.

6. CONSIDERAÇÕES FINAIS

O sharenting é um fenômeno contemporâneo e, quando realizado dentro de certos limites, constitui uma maneira legítima do exercício da liberdade de expressão por parte dos pais, que não podem, simplesmente, ser impedidos de compartilhar informações a respeito de seus filhos.

Contudo, considerando-se os riscos decorrentes da exposição exagerada de informações sobre as crianças na internet, assim como os interesses também legítimos das crianças em relação à privacidade (os quais podem vir à tona apenas quando a criança atinge certo grau de maturidade), é necessário que sejam adotadas medidas que controlem esse comportamento.

Como a proteção de dados pessoais, a privacidade, o direito ao esquecimento e a garantia à liberdade de expressão constituem direitos fundamentais, nenhuma medida pode ser adotada de modo a suprimi-los por

57 “Policy makers and the industry face the challenge of not just including as much information as possible, but of increasing the chance that parents might read and use the privacy statement in a way that is beneficial to their children.” STANALAND, Andrea J. S.; LWIN, May O.; LEONG, Susanna. Providing Parents with Online Privacy Information: Approaches in the US and the UK. *The Journal Of Consumer Affairs*, v. 43, p. 474-494, 2009. p. 490.

58 Tecnicamente o direito ao esquecimento pode ser viabilizado. Uma das inúmeras possibilidades técnicas é explicada por Lima: “as ferramentas tecnológicas, como exemplo, um metadado que adiciona uma informação ao dado para que seja acessível apenas por um prazo de validade, como o aplicativo Snapchat, podem viabilizar o esquecimento, o que pode ser utilizado e difundido na sociedade como um todo” LIMA, Cíntia Rosa Pereira de. Direito ao Esquecimento e Internet: o fundamento legal no Direito Comunitário europeu, no Direito italiano e no Direito brasileiro. *Revista dos Tribunais*, v. 946, p.77-109, ago. 2014.

inteiro. As possíveis soluções devem buscar, na maior medida possível, a realização de todos os interesses envolvidos.

Dentre as possibilidades analisadas ao longo do texto, pode-se dizer que seriam importantes políticas públicas para educação em relação ao uso das ferramentas digitais. Essas políticas podem ser executadas pelo próprio Estado (propaganda e divulgação de material educativo para adultos e crianças) e, também, pelas empresas que exploram as atividades econômicas ligadas ao sharenting (como as redes sociais e as ferramentas de busca).

Especificamente em relação às aplicações de internet, considerando-se que elas criam o ambiente para que o sharenting ocorra e que, também, criam expectativas de segurança em relação aos dados pessoais, é necessário que, de algum modo, a sua conduta ajude a prevenir e corrigir a eventual superexposição de informações de crianças, ainda que realizada por seus pais ou responsáveis legais.

A construção do caminho no Brasil para proteção dos interesses das crianças com a preservação dos demais interesses envolvidos pode decorrer tanto de uma evolução legislativa (implementação de um marco legal específico para proteção de dados) quanto da evolução no entendimento jurisprudencial, de modo que sejam efetivadas medidas concretas pelos provedores, especialmente no que tange às obrigações de informação e à implementação de mecanismos técnicos para viabilizar o direito ao esquecimento.

REFERÊNCIAS

ACIOLI, Bruno de Lima; EHRHARDT JÚNIOR, Marcos Augusto de Albuquerque. Uma agenda para o direito ao esquecimento no Brasil. *Revista Brasileira de Políticas Públicas*, v. 7, n. 3, 2017.

ALEXY, Robert. *Teoria dos Direitos Fundamentais*. São Paulo: Malheiros, 2012.

ALLEN, Anita L. Protecting one's own privacy in a big data economy. *Harvard Law Review*, v. 130, p. 71-78, dez. 2016.

BARTOLI, Emmanuelle. Children's data protection vs marketing companies. *International Review Of Law, Computers & Technology*, v. 23, n. 1-2, p. 35-45, jul. 2009. Informa UK Limited. <http://dx.doi.org/10.1080/13600860902742612>.

BESSANT, Claire. Data protection, safeguarding and the protection of children's privacy: exploring local authority guidance on parental photography at school events. *Information & Communications Technology Law*, v. 23, n. 3, p. 256-272, 2 set. 2014. Informa UK Limited. <http://dx.doi.org/10.1080/13600834.2014.973178>.

BRASIL. Superior Tribunal de Justiça. AgInt no Recurso Especial n. 1.593.873-SP. Agravante: Google Brasil Internet Ltda. Relatora: Ministra Nancy Andrighi. Brasília, DF, 10 de novembro de 2016. *DJe*. Brasília, 17 nov. 2016.

BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 74.473-RJ. Recorrentes: Edenir dos Santos Mario e Outros. Relator: Ministro Sálvio de Figueiredo Teixeira. Brasília, DF, 25 de fevereiro de 1999. *DJ*. Brasília, 21 jun. 1999.

BRASIL. Supremo Tribunal Federal. Acórdão n° 2144-3. Paciente: Siegfried Ellwanger. Relator: Ministro Maurício Corrêa. Brasília, DF, 17 de setembro de 2003. *DJ*. Brasília, 19 mar. 2004.

CANARIS, Claus-Wilhelm. *Pensamento Sistemático e Conceito de Sistema na Ciência do Direito*. 3. ed. Lisboa: Fundação Calouste Gulbenkian, 2002.

CHEHAB, Gustavo Carvalho. O direito ao esquecimento na sociedade da informação. In: CLÈVE, Clèmerson Merlin. *Doutrinas Essenciais de Direito Constitucional*. São Paulo: Revista dos Tribunais, 2015. p. 563-596.

COLOMBO, Cristiano; FACCHINI NETO, Eugênio. Ciberespaço e conteúdo ofensivo gerado por terceiros: a proteção dos direitos de personalidade e a responsabilização civil dos provedores de aplicação, à luz da jurisprudência do Superior Tribunal de Justiça. *Revista Brasileira de Políticas Públicas*, v. 7, n. 3, 2017.

ERDOS, David. Delimiting the Ambit of Responsibility of Intermediary Publishers for Third Party Rights in European Data Protection: Towards a Synthetic Interpretation of the EU acquis. *University of Cambridge Faculty of Law Research Paper No. 31/2017*, Cambridge, 27 jun. 2017. Disponível em: <<https://ssrn.com/abstract=2993154>>. Acesso em: 21 ago. 2017.

LIMA, Cíntia Rosa Pereira de. Direito ao Esquecimento e Internet: o fundamento legal no Direito Comunitário europeu, no Direito italiano e no Direito brasileiro. *Revista dos Tribunais*, v. 946, p.77-109, ago. 2014.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MOREIRA, Rodrigo Pereira; MEDEIROS, Jaqueline Souza. Direito ao Esquecimento: Entre a Sociedade da Informação e a Civilização do Espetáculo. *Revista de Direito Privado*, v. 70, p. 71-98, 2016.

NAIR, Abhilash. Mobile phones and the internet: Legal issues in the protection of children. *International Review Of Law, Computers & Technology*, v. 20, n. 1-2, p. 177-185, mar. 2006. Informa UK Limited. <http://dx.doi.org/10.1080/13600860600579779>.

NISHIYAMA, Adolfo Mamoru; DENSA, Roberta. A Proteção dos Consumidores Hipervulneráveis: os portadores de deficiência, os idosos, as crianças e os adolescentes. *Revista de Direito do Consumidor*, v. 76, p. 13-45, out./dez. 2010.

OSWALD, Marion; JAMES, Helen; NOTTINGHAM, Emma. The not-so-secret life of five-year-olds: legal and ethical issues relating to disclosure of information and the depiction of children on broadcast and social media. *Journal Of Media Law*, v. 8, n. 2, p. 198-228, 13 out. 2016. Informa UK Limited. <http://dx.doi.org/10.1080/17577632.2016.1239942>.

ROCHA, Maria Vital da; CUNHA, Isaac Rodrigues; OLIVEIRA, Karin de Fátima Rodrigues. Esquecimento, internet e “preferência” da informação: possibilidades de aplicação da doutrina dos preferred rights da jurisprudência norte-americana ao caso brasileiro. *Revista Brasileira de Políticas Públicas*, v. 7, n. 3, 2017.

SCHREIBER, Anderson. *Direitos da Personalidade*. São Paulo: Atlas, 2011.

SIMPSON, Brian. Tracking children, constructing fear: GPS and the manufacture of family safety. *Information & Communications Technology Law*, v. 23, n. 3, p. 273-285, 2 set. 2014. Informa UK Limited. <http://dx.doi.org/10.1080/13600834.2014.970377>.

STANALAND, Andrea J. S.; LWIN, May O.; LEONG, Susanna. Providing Parents with Online Privacy Information: Approaches in the US and the UK. *The Journal Of Consumer Affairs*, v. 43, p. 474-494, 2009.

STEINBERG, Stacey B. Sharenting: Children’s privacy in the age of social media. *Emory Law Journal*, Atlanta, v. 66, p. 839-884, 2017. Disponível em: <<http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1796&context=facultypub>>. Acesso em: 21 ago. 2017.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. *Acórdão nº C-131/12*. Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González. Luxemburgo, 2014. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT>>. Acesso em: 09 set. 2017.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. *Acórdão nº C-101/01*. Bodil Lindqvist. Luxemburgo, 2003. Disponível em: <<http://curia.europa.eu/juris/showPdf.jsf?jsessionid=9ea7d2dc30dd28296b2724ac4b0895cf91c3f2a490df.e34KaxiLc3qMb40Rch0SaxuSaxb0?docid=48382&pageIndex=0&doclang=PT&dir=&occ=first&part=1&cid=161864>>. Acesso em: 14 set. 2017.

VIANA, Janile Lima; MAIA, Cinthia MANESES; ALBUQUERQUE, Paulo Germano Barrozo de. O cyberbullying e os limites da liberdade de expressão. *Revista Brasileira de Políticas Públicas*, v. 7, n. 3, 2017.

VIANA, Rafael Souza; SANTANA, Héctor Valverde. O compartilhamento de dados e informações pessoais de consumidores: o abuso dos fornecedores e as propostas apresentadas no PLS 181/2014. *Revista Brasileira de Políticas Públicas*, v. 7, n. 1, p. 238-253, 8 maio 2017. <http://dx.doi.org/10.5102/rbpp.v7i1.4579>.

Para publicar na revista Brasileira de Políticas Públicas, acesse o endereço eletrônico www.rbpp.uniceub.br
Observe as normas de publicação, para facilitar e agilizar o trabalho de edição.